SECURITY MANAGEMENT DEVICES

Patent Number: JP7262135
Publication date: 1995-10-13

Inventor(s): SAITO YOKO
Applicant(s): HITACHI LTD

Requested Patent: ⌜ JP7262135
Application Priority Number(s): JP19940047194 19940317
IPC Classification: G06F15/00; G06F1/00; G06F13/00; H04L9/00; H04L9/10;
EC Classification:
Equivalents:

Abstract

PURPOSE:To cope with an infringement of security that a wrong intruder from one system wrongfully accesses another system in open systems.
CONSTITUTION:At least one or more security audit server (SO) is provided in open distributed network systems (SS1, SS2, SS3...) and this SO always extracts and analyzes security messages (M1, etc.) which are transmitted from work stations (WS11, etc.) connected to networks and are related to the infringement of security and collects and accumulates the results. In the case of the message which may have an influence upon systems, a security report related to this message is generated. All security reports are synthetically analyzed to diagnose the weak points of systems, and the proper change of the security policy is requested to actual systems.

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平7－262135

(43)公開日　平成７年(1995)10月13日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	15/00	３３０　Ａ	7459－5L		
	1/00	３７０　Ｅ			
	13/00	３５１　Ｚ	7368－5B		
Ｈ０４Ｌ	9/00				
				Ｈ０４Ｌ　9/ 00　Ｚ	

審査請求　未請求　請求項の数３　ＯＬ　（全 10 頁）　最終頁に続く

(21)出願番号　特願平6－47194

(22)出願日　平成６年(1994)３月17日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　齋藤　洋子
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

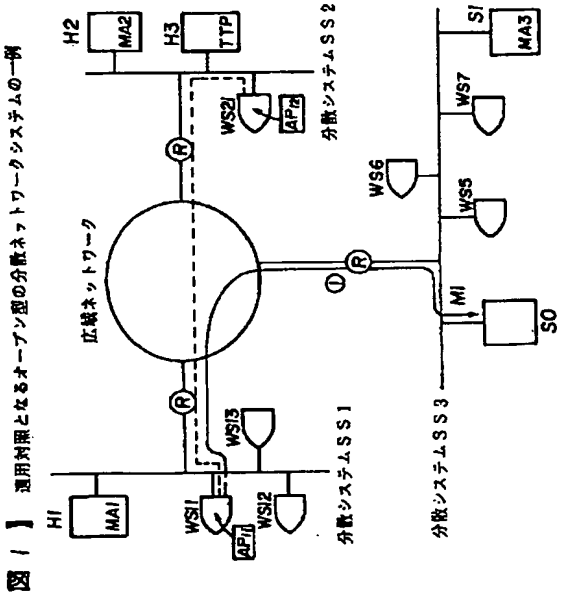
(74)代理人　弁理士　武　顕次郎

(54)【発明の名称】　セキュリティ管理装置

(57)【要約】

【目的】　セキュリティ管理装置に関し、オープンシステムにおいて他のシステムからの不正侵入者が別のシステムへ不正アクセスするタイプのセキュリティ侵害に対処できるようにする。

【構成】　オープン型の分散ネットワークシステム(SS1, SS2, SS3...)に少なくとも一以上のセキュリティオーディットサーバ(S0)を設ける。セキュリティオーディットサーバ(S0)は、ネットワークに接続されたＷＳ(WS11など)から発信されるセキュリティ侵害に関するセキュリティメッセージ(M1など)を常時抽出して分析し、その結果をまとめて集積する。そして、システムへの影響が懸念されるメッセージがあった場合には、当該メッセージに関するセキュリティレポートを作成する。さらに、すべてのセキュリティレポートを統合的に分析してシステムの弱点を診断し、実システムに対して適切なセキュリティポリシーの改変要求を行う。



【図１】

1

【特許請求の範囲】

【請求項1】　複数の処理装置が接続されており、所定のセキュリティポリシーに基づいて運用管理が行われる分散ネットワークシステムにおいて、少なくともひとつのセキュリティオーディットサーバを設け、

前記処理装置内で動作中のアプリケーションから出力されたセキュリティメッセージの抽出を行うセキュリティメッセージ抽出手段と、

抽出された前記セキュリティメッセージを前記セキュリティポリシーと照合して、前記セキュリティメッセージに対応する前記アプリケーションの処理の正当性についての分析を行うセキュリティメッセージ分析手段と、

前記セキュリティメッセージ分析手段による分析結果をまとめて前記セキュリティオーディットサーバに蓄積するセキュリティメッセージ集積手段とを具備する構成としたことを特徴とするセキュリティ管理装置。

【請求項2】　同一のセキュリティポリシーを有する複数の前記ネットワークシステムを相互接続して構成されたオープン型の分散ネットワークシステムにおいて、ネットワークシステムをまたがったセキュリティ管理を行うためにＴＴＰを設け、

前記セキュリティメッセージ分析手段によって正当性なしと判定されたセキュリティメッセージに関連する情報の選択収集を行うセキュリティメッセージ選択収集手段と、

前記セキュリティメッセージ選択収集手段によって選択収集された一以上の前記セキュリティメッセージに基づいてセキュリティレポートを作成するセキュリティレポート作成手段とを具備する構成としたことを特徴とする請求項1記載のセキュリティ管理装置。

【請求項3】　個別に生成された一以上の前記セキュリティレポートを統合的に分析し、前記セキュリティポリシーの評価を行うセキュリティレポート分析手段と、

前記セキュリティレポート分析手段による前記セキュリティポリシーの評価に基づいて前記セキュリティポリシーの問題点を明確化するとともに、前記問題点を解消させるための前記セキュリティポリシーの改変案を作成するセキュリティポリシー診断手段と、

前記セキュリティポリシーの改変案に基づいて、相互接続された前記ネットワークシステムのそれぞれに対して前記セキュリティポリシーの改変要求を行うセキュリティポリシー改変要求手段とを具備する構成としたことを特徴とする請求項2記載のセキュリティ管理装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明はセキュリティ管理装置に係り、特に、オープンシステムにおいて他のシステムからの不正侵入者が別のシステムへ不正アクセスするタイプのセキュリティ侵害に対処することが可能なセキュリティ管理装置に関する。

2

【0002】

【従来の技術】近年、複数のネットワークシステムを介して接続される複数のＷＳ（ワークステーション）の間で処理が行われるＥＤＩ(Electronic Data Interchange)、あるいは、ＥＦＴ(Electronic Funds Transfer)などのコンピュータシステムを用いた電子取引が普及してきている。上記のようなオープンシステムでは、他のシステムからの不正侵入者が別のシステムへ不正アクセスするタイプのセキュリティ侵害が脅威となるが、そこで、ISO SC21/WG4等のＯＳＩ管理のプロジェクトでは、セキュリティに関連するメッセージを他の機器障害情報と同様にネットワークマネジャに管理させようとする試みがなされている。

【0003】その一方、ネットワークのセキュリティに関連する障害管理を考慮した技術として、①往復トラフィック不均衡と交換機内の情報喪失状況を区別する技術（特開平3-167939号公報に記載）や、②セキュリティ管理をネットワークシステム上のひとつの機器で行うことによって機密保持の信頼性を向上させる技術（特開平5－22310）などが提案されている。

【0004】

【発明が解決しようとする課題】しかしながら、ネットワークシステムを介して接続されたオープンな異機種の分散システム環境では、必ずしも「自己管理」されているシステムとは限らないため、セキュリティ管理が非常に難しい。例えば、ＯＳＩ管理に基づくネットワークマネジャは、その管理するドメイン内の通信についてはセキュリティ管理できるが、管理するドメイン外部からのアクセスについてはセキュリティ管理できない。すなわち、閉じた自己管理されたシステムを対象としている上記従来技術では、オープンな異機種の分散システム環境でのセキュリティ管理に対応することができないという問題点があった。

【0005】そこで、ISO/IEC DC10181-7 セキュリティオーディットフレームワークでは、ネットワークシステムに発生したセキュリティ侵害事象に関するアラームを分析する基本的なモデルが検討されている。また、オープンな異機種の分散システム環境において、管理ドメイン間をまたがった部分でのセキュリティ管理に対応することができるモデルのひとつとして、ＯＳＩ管理に基づく各々のネットワークマネジャのドメインを越えた部分のセキュリティについてＴＴＰ（Trusted Third Party：信頼できる第三者機関）に管理を委託するモデルの概念が提唱されている。しかし、上記モデルでは、異なる複数のネットワークシステムに発生したセキュリティ侵害事象を監査する機能を分散システム環境でどのように実装するのか、また、セキュリティ侵害の監査結果をセキュリティポリシーにどのように反映させるのか、その方法については何も具体的に提案されていない。

【0006】したがって本発明の目的は、上記の問題点

3

を解決して、上記ＴＴＰが持つべき機能を具体化して、オープンな異機種の分散システム環境に対応できるセキュリティ管理装置を提供することにある。

【０００７】

【課題を解決するための手段】

(1) 上記の目的を達成するため、本発明のセキュリティ管理装置は、複数の処理装置が接続されており、所定のセキュリティポリシーに基づいて運用管理が行われる分散ネットワークシステムにおいて、少なくともひとつのセキュリティオーディットサーバを設け、前記処理装置内で動作中のアプリケーションから出力されたセキュリティメッセージの抽出を行うセキュリティメッセージ抽出手段と、抽出された前記セキュリティメッセージを前記セキュリティポリシーと照合して、前記セキュリティメッセージに対応する前記アプリケーションの処理の正当性についての分析を行うセキュリティメッセージ分析手段と、前記セキュリティメッセージ分析手段による分析結果をまとめて前記セキュリティオーディットサーバに蓄積するセキュリティメッセージ集積手段とを具備する構成としたものである。

【０００８】(2) また、さらに、(1)の構成に加えて、同一のセキュリティポリシーを有する複数の前記ネットワークシステムを相互接続して構成されたオープン型の分散ネットワークシステムにおいて、ネットワークシステムをまたがったセキュリティ管理を行うためにＴＴＰを設け、前記セキュリティメッセージ分析手段によって正当性なしと判定されたセキュリティメッセージに関連する情報の選択収集を行うセキュリティメッセージ選択収集手段と、前記セキュリティメッセージ選択収集手段によって選択収集された一以上の前記セキュリティメッセージに基づいてセキュリティレポートを作成するセキュリティレポート作成手段とを具備する構成としたものである。

【０００９】(3) また、さらに、(2)の構成に加えて、個別に生成された一以上の前記セキュリティレポートを統合的に分析し、前記セキュリティポリシーの評価を行うセキュリティレポート分析手段と、前記セキュリティレポート分析手段による前記セキュリティポリシーの評価に基づいて前記セキュリティポリシーの問題点を明確化するとともに、前記問題点を解消させるための前記セキュリティポリシーの改変案を作成するセキュリティポリシー診断手段と、前記セキュリティポリシーの改変案に基づいて、相互接続された前記ネットワークシステムのそれぞれに対して前記セキュリティポリシーの改変要求を行うセキュリティポリシー改変要求手段とを具備する構成としたものである。

【００１０】

【作用】上記構成に基づく作用を説明する。

【００１１】(1) 本発明のセキュリティ管理装置では、複数の処理装置が接続されており、所定のセキュリティ

4

ポリシーに基づいて運用管理が行われる分散ネットワークシステムにおいて、少なくともひとつのセキュリティオーディットサーバを設け、前記処理装置内で動作中のアプリケーションから出力されたセキュリティメッセージの抽出を行うセキュリティメッセージ抽出手段と、抽出された前記セキュリティメッセージを前記セキュリティポリシーと照合して、前記セキュリティメッセージに対応する前記アプリケーションの処理の正当性についての分析を行うセキュリティメッセージ分析手段と、前記セキュリティメッセージ分析手段による分析結果をまとめて前記セキュリティオーディットサーバに蓄積するセキュリティメッセージ集積手段とを具備する構成としたことにより、ネットワークにおけるセキュリティ侵害の兆候を示すメッセージをあらかじめセキュリティメッセージとして定義しておけば、当該セキュリティメッセージのみを他のメッセージと区別して収集し、収集された一以上のセキュリティメッセージを分析してセキュリティ侵害の可能性の有無をチェックし、分析結果を実際のセキュリティ侵害に関わる記録として蓄積する、という一連の作業が常時自動的に行われるので、ネットワークの運用中におけるセキュリティの状態がオーディットサーバによって常に監視および記録され、万一のセキュリティ侵害への対処に必要な情報を容易かつ効率的に得ることができる。

【００１２】(2) また、さらに、(1)の構成に加えて、同一のセキュリティポリシーを有する複数の前記ネットワークシステムを相互接続して構成されたオープン型の分散ネットワークシステムにおいて、ネットワークシステムをまたがったセキュリティ管理を行うためにＴＴＰを設け、前記セキュリティメッセージ分析手段によって正当性なしと判定されたセキュリティメッセージに関連する情報の選択収集を行うセキュリティメッセージ選択収集手段と、前記セキュリティメッセージ選択収集手段によって選択収集された一以上の前記セキュリティメッセージに基づいてセキュリティレポートを作成するセキュリティレポート作成手段とを具備する構成としたことにより、あるネットワーク中でセキュリティ侵害に関連する操作を行った着目ユーザを特定し、他のネットワークにおける当該着目ユーザのセキュリティ侵害に関する記録をチェックし、オープン型の分散ネットワークシステム全域における当該着目ユーザに関する個別のセキュリティレポートを作成する、という一連の作業が自動的に行われるので、オープン型の分散ネットワークシステム全域における当該着目ユーザ（あるいは当該着目ユーザのユーザＩＤを盗用した者）によるセキュリティ侵害の前歴情報を容易かつ効率的に得ることができる。

【００１３】(3) また、さらに、(2)の構成に加えて、個別に生成された一以上の前記セキュリティレポートを統合的に分析し、前記セキュリティポリシーの評価を行うセキュリティレポート分析手段と、前記セキュリティレ

5

ポート分析手段による前記セキュリティポリシーの評価に基づいて前記セキュリティポリシーの問題点を明確化するとともに、前記問題点を解消させるための前記セキュリティポリシーの改変案を作成するセキュリティポリシー診断手段と、前記セキュリティポリシーの改変案に基づいて、相互接続された前記ネットワークシステムのそれぞれに対して前記セキュリティポリシーの改変要求を行うセキュリティポリシー改変要求手段とを具備する構成としたことにより、過去に何度も報告されたことのあるセキュリティ侵害など、あらかじめ予測可能なセキュリティ侵害については、セキュリティポリシーの問題点を容易に指摘して、当該セキュリティ侵害に対して有効なセキュリティポリシーの改変案を分散ネットワークシステムに対して自動的に提示することができる。

【００１４】

【実施例】以下、本発明のセキュリティ管理装置の一実施例を図面を用いて詳細に説明する。

【００１５】図１は、本発明のセキュリティ管理装置の適用対象となるオープン型の分散ネットワークシステムの一例を示す図であり、Ｓ０はセキュリティオーディットサーバ、Ｓ１，Ｓ２，....はサーバ、Ｈ１，Ｈ２，....はホストシステム、WS１，WS２，....はワークステーション、SS１，SS２，....は分散システム、MA１，MA２，MA３はネットワークマネジャ、AP１，AP２，....はアプリケーションプログラム、ＴＴＰ（Trusted Third Party）は“信頼できる第三者機関”、Ｍ１はセキュリティ侵害メッセージ、Ｒはセキュリティレポートをそれぞれ示す。

【００１６】図１において、一以上のホストシステム（Ｈ１，Ｈ２，....），サーバ（Ｓ１，Ｓ２，....），ワークステーション（WS１，WS２，....）と、セキュリティオーディットサーバＳ０とが支線ＬＡＮに接続され、それぞれ独立した分散システム（SS１，SS２，....）を構築している。そして、各分散システムは超高速な広域網，各種業者ＶＡＮ，業界固有のネットワークなどを介して相互に接続され、これによってオープン型の分散ネットワークシステムが形成される。なお、オープン型の分散ネットワークシステムにおいては、異機種間の接続が可能である。

【００１７】また、図１に示したオープン型の分散ネットワークシステムは、あらかじめ定められたシステム全体のセキュリティポリシー（安全保護方針）に基づいて運用される。例えば、一般的なオープン型の分散ネットワークシステムでは、次に示すようなセキュリティポリシーが定められていることが多い。

(1) 各分散システムにおいては、ユーザが支線ＬＡＮ上に接続されたWSから他のWSあるいはホストシステムにログインする際に、当該ユーザの識別および認証を必ず実施しなければならない（これに伴って、認証サーバを設けなければならない。）。

6

(2) WSを使用中のユーザやWS上で動作中のアプリケーションがネットワーク上のデータベースサーバなどに対するアクセスを開始する場合には、当該アクセスが正当なものであるか否かを判定して、アクセス制御を実施しなければならない。

(3) 分散システムおよび広域網の両方を通信に使用するなど、複数のネットワークを経由する通信の場合には、当事者以外の者に通信内容を知られないようにする機能や、通信内容を保全する機能を設けなければならない（これに伴って、鍵管理サーバを設けなければならない。）。

(4) セキュリティに関連して発生する全事象の履歴情報を記録するとともに、セキュリティ侵害があったときにその事実の報告および内容の分析を行うオーディット機能を設けなければならない。

【００１８】すなわち、上述したセキュリティ機能がすべて実装されて初めて、オープン型の分散ネットワークシステムの管理体制が完全なものになったということができる。本実施例の以後の説明においては、上記のシステムにおける④のオーディット機能について解説を行う。

【００１９】本発明のセキュリティ管理装置は、分散ネットワークシステム内にセキュリティオーディットサーバを設け、これによってセキュリティ侵害事象の検出からセキュリティレポートの作成までのすべてを行うことを目的とする。例えば図１において、分散システムSS１に属するWS１１で動作中のAP１１と、分散システムSS２に属するWS２１で動作中のAP２１とが通信を行っているとき、WS１１側でセキュリティ侵害事象が検出されると、WS１１においてセキュリティ侵害報告メッセージＭ１が作成され、セキュリティオーディットサーバＳ０に送信される（図１中の①で示す矢印線がセキュリティ侵害報告メッセージＭ１の流れを示す）。

【００２０】図２は、本発明のセキュリティ管理装置におけるセキュリティポリシーの一例を示す図である。図２（ａ）において、複数の分散システムにまたがるネットワーク全体のセキュリティ管理は、あらかじめすべての分散システム間で共通に定められたセキュリティポリシーＰに基づき、ＴＴＰ（Trusted Third Party)によって実施されるので、世界的に共通な表現方法やセキュリティ評価基準として規定しておくことが望ましい。セキュリティポリシーＰの定義は、図２に示すように、認証レベル，アクセス制御レベル，完全性レベル，機密性レベル，オーディットレベルなどのセキュリティポリシーＰを構成する各パラメタの値を設定することによって行う。例えば図２（ｂ）においては、ユーザＵ１のセキュリティ管理を行うためのセキュリティポリシーP_{u1}が次のように定義されている。

・認証レベル　Au＝２

定期的に認証処理を行う必要があることを示し、ユーザ

7

は定期的にパスワードを投入することを義務づけられている。

・アクセス制御レベル　Ac＝２

他の分散システムの範囲まで含めて、アクセス制御を行うことができる。

(etc.)

上記の場合において、WS１１からアクセス中のユーザＵ１に義務付けられた定期的なパスワードの確認が実施されなかった場合には、本来のユーザＵ１が端末から離れている隙をついて侵入者がWS１１を使用しているという可能性や、ユーザＵ１のパスワードを盗んだ第三者がネットワークシステムに侵入している可能性などが考えられるので、WS１１は、これをセキュリティ侵害事象が発生したものとみなす。そしてWS１１は、セキュリティポリシーP_{U1}の規定に違反しているユーザＵ１の操作（上記ではパスワードを定期的に投入しなかったこと）についてセキュリティ侵害事象の可能性を指摘するメッセージＭ１を作成し、図１中の①の通信経路でセキュリティオーディットサーバＳ０に対する送信を行う。

【００２１】図３は、本発明のセキュリティ管理装置の一実施例を構成するセキュリティメッセージ抽出手段による処理の概要を示す図であり、図３（ａ）は前述したWS１１においてセキュリティ侵害を検出してからメッセージＭ１を送信するまでの処理シーケンスを、図３（ｂ）はメッセージＭ１を受信した後のオーデットサーバＳ０の処理フローを、それぞれ表わす。すなわち、オーデットサーバＳ０は、メッセージＭ１の発信元の正当性が確認された後に、受信したメッセージＭ１の分析処理を開始する。

【００２２】図４は、本発明のセキュリティ管理装置の一実施例を構成するセキュリティメッセージ分析手段による処理の概要を示す図であり、図４（ａ）はセキュリティメッセージの分析に必要なセキュリティポリシーの要求処理シーケンスを、図４（ｂ）はセキュリティポリシーに対するセキュリティメッセージの比較対照処理を、それぞれ表わす。すなわち図４（ａ）において、前述したようにＴＴＰがユーザＵ１に関するセキュリティポリシーP_{U1}を管理しているため、オーディットサーバＳ０は、ＴＴＰに対してP_{U1}の情報提供の要求を行う。そして図４（ｂ）において、ユーザＵ１に関するセキュリティポリシーP_{U1}を獲得した後、オーディットサーバＳ０は、実際にメッセージＭ１の内容がP_{U1}で規定されている内容に違反しているか否かを確認し、違反が確認された場合には当該ユーザＵ１についてのメッセージ選択収集処理を行う。

【００２３】図５は、本発明のセキュリティ管理装置の一実施例を構成するセキュリティメッセージ選択収集手段による処理の概要を示す図であり、図５（ａ）はユーザＵ１に関する情報要求の処理シーケンスを、図５（ｂ）は同じく処理フローを、それぞれ表わす。すなわち図５（ａ）において、ユーザＵ１が分散システムSS１およびSS２へのアクセス権限を有するため、上記システムのネットワークマネジャMA１およびMA２に対してユーザＵ１に関する情報要求を行う。また図５（ｂ）において、オーディットサーバＳ０は、セキュリティポリシーP_{U1}の情報に基づいてユーザＵ１がアクセス可能な他の分散システムSSｎを調査し、当該システムSSｎのマネジャーMAｎにセキュリティ情報の報告を要求して獲得された情報に対して、メッセージ集積処理を行う。

8

【００２４】図６は、本発明のセキュリティ管理装置の一実施例を構成するセキュリティメッセージ集積手段による処理の概要を示す図である。同図中、オーディットサーバＳ０は、前述したセキュリティメッセージ選択収集手段によって獲得されたユーザＵ１に関するすべての履歴情報を、時系列，アクセス頻度，あるいはアクセス内容などの項目をキーとしてソートした後、オーディットサーバＳ０内のオーディットトレイルに格納する。

【００２５】図７は、図３～図６の各処理の対象とされるデータ群の形式の一例を示す図であり、図７（ａ）はセキュリティメッセージの形式を、図７（ｂ）はセキュリティメッセージ分析手段によるセキュリティメッセージＭ１の分析結果の形式を、図７（ｃ）はセキュリティメッセージ集積手段によって分散システムごとに蓄積されたセキュリティメッセージの履歴情報の形式を、図７（ｄ）はセキュリティメッセージ選択収集手段によってまとめられたユーザＵ１に関する履歴情報の形式を、図７（ｅ）はセキュリティレポート作成手段によって作成されたセキュリティレポートの形式を、それぞれ表わす。図７（ｅ）においては、ユーザＵ１についてアクセス日時，アクセス先，セキュリティポリシーＵ１に対する違反の有無が、セキュリティレポートとしてまとめられている。

【００２６】以上のように、セキュリティオーディットサーバＳ０は、セキュリティメッセージＭ１の抽出，分析，集積を行う。そして、セキュリティ侵害の内容を分析して重大な侵害と判断したり、P_{U1}の値から他の分散システムへの影響ありと判断した場合には、分散システムSS１，SS２，SS３に蓄積されている多数のセキュリティメッセージの中から、セキュリティメッセージＭ１を発生させたユーザＵ１に関連するメッセージを選択収集および集積して、メッセージＭ１すなわちユーザＵ１に関するセキュリティレポートを作成する。

【００２７】図８は、本発明のセキュリティ管理装置の一実施例を構成するセキュリティレポート分析手段およびセキュリティポリシー診断手段による処理の概要を示す図であり、図８（ａ）はセキュリティレポート分析手段およびセキュリティポリシー診断手段の処理シーケンスを、図８（ｂ）はＴＴＰの動作処理フローを、それぞれ表わす。図８（ａ）において、ＴＴＰは、ネットワークシステム内のセキュリティオーディットサーバＳ０か

9

らセキュリティレポートが報告されてくると、その内容を分析して、セキュリティオーディットサーバＳ０に分析結果を返答する。図８（ｂ）において、ＴＴＰは、セキュリティレポートの内容が通信途上で改竄されていないか、あるいはその内容を信頼できるか否かというデータの正当性を判定する。そして、改竄された様子がなく、内容を信頼できると判定した場合には、セキュリティポリシーの内容をチェックして、ユーザＵ１に関するセキュリティポリシーP_{U1}の上記セキュリティレポートによって示されるセキュリティ侵害に対する弱点を診断した後、この弱点を克服するために必要なセキュリティポリシーP_{U1}の改変案を作成する。例えば、セキュリティレポートの内容に基づいてセキュリティポリシーをチェックした結果、ユーザＵ１に対しては、分散システムSS１およびSS２内部のデータをあまり公開すべきではないと判定した場合には、P_{U1}のアクセス制御レベルを１に変更してユーザＵ１の分散システムSS１およびSS２へのアクセスそのものを禁止するか、あるいは機密性レベルをより高く設定してデータの盗み見を許さないようにする、という２通りの改革案が考えられる。

【００２８】図９は、本発明のセキュリティ管理装置の一実施例を構成するセキュリティポリシー改変要求手段による処理の概要を示す図である。図９において、ＴＴＰは、P_{U1}の改変要求を各々の分散システムにおけるネットワークマネジャMA１，MA２，MA３に通知し、これらのマネジャで管理している管理オブジェクト情報の改変を要求する。例えば、P_{U1}を改変してユーザＵ１から発信される情報に対して暗号処理を行うことを義務づける場合には、ユーザＵ１との通信を行うMA１，MA２，MA３内のオブジェクトのそれぞれについて鍵情報を設定するように改変要求を行う。

【００２９】

【発明の効果】

(1) 以上詳しく説明したように、本発明のセキュリティ管理装置によれば、複数の処理装置が接続されており、所定のセキュリティポリシーに基づいて運用管理が行われる分散ネットワークシステムにおいて、少なくともひとつのセキュリティオーディットサーバを設け、前記処理装置内で動作中のアプリケーションから出力されたセキュリティメッセージの抽出を行うセキュリティメッセージ抽出手段と、抽出された前記セキュリティメッセージを前記セキュリティポリシーと照合して、前記セキュリティメッセージに対応する前記アプリケーションの処理の正当性についての分析を行うセキュリティメッセージ分析手段と、前記セキュリティメッセージ分析手段による分析結果をまとめて前記セキュリティオーディットサーバに蓄積するセキュリティメッセージ集積手段とを具備する構成としたことにより、ネットワークにおけるセキュリティ侵害の兆候を示すメッセージをあらかじめセキュリティメッセージとして定義しておけば、当該セキュリティメッセージのみを他のメッセージと区別して収集し、収集された一以上のセキュリティメッセージを分析してセキュリティ侵害の可能性の有無をチェックし、分析結果を実際のセキュリティ侵害に関わる記録として蓄積する、という一連の作業が常時自動的に行われるので、ネットワークの運用中におけるセキュリティの状態がオーディットサーバによって常に監視および記録され、万一のセキュリティ侵害への対処に必要な情報を容易かつ効率的に得ることができるという効果が得られる。

10

【００３０】(2) また、さらに、(1)の構成に加えて、同一のセキュリティポリシーを有する複数の前記ネットワークシステムを相互接続して構成されたオープン型の分散ネットワークシステムにおいて、ネットワークシステムをまたがったセキュリティ管理を行うためにＴＴＰを設け、前記セキュリティメッセージ分析手段によって正当性なしと判定されたセキュリティメッセージに関連する情報の選択収集を行うセキュリティメッセージ選択収集手段と、前記セキュリティメッセージ選択収集手段によって選択収集された一以上の前記セキュリティメッセージに基づいてセキュリティレポートを作成するセキュリティレポート作成手段とを具備する構成としたことにより、あるネットワーク中でセキュリティ侵害に関連する操作を行った着目ユーザを特定し、他のネットワークにおける当該着目ユーザのセキュリティ侵害に関する記録をチェックし、オープン型の分散ネットワークシステム全域における当該着目ユーザに関する個別のセキュリティレポートを作成する、という一連の作業が自動的に行われるので、オープン型の分散ネットワークシステム全域における当該着目ユーザ（あるいは当該着目ユーザのユーザＩＤを盗用した者）によるセキュリティ侵害の前歴情報を容易かつ効率的に得ることができるという効果が得られる。

【００３１】(3) また、さらに、(2)の構成に加えて、個別に生成された一以上の前記セキュリティレポートを統合的に分析し、前記セキュリティポリシーの評価を行うセキュリティレポート分析手段と、前記セキュリティレポート分析手段による前記セキュリティポリシーの評価に基づいて前記セキュリティポリシーの問題点を明確化するとともに、前記問題点を解消させるための前記セキュリティポリシーの改変案を作成するセキュリティポリシー診断手段と、前記セキュリティポリシーの改変案に基づいて、相互接続された前記ネットワークシステムのそれぞれに対して前記セキュリティポリシーの改変要求を行うセキュリティポリシー改変要求手段とを具備する構成としたことにより、過去に何度も報告されたことのあるセキュリティ侵害など、あらかじめ予測可能なセキュリティ侵害については、セキュリティポリシーの問題点を容易に指摘して、当該セキュリティ侵害に対して有効なセキュリティポリシーの改変案を分散ネットワーク

11

システムに対して自動的に提示することができるという効果が得られる。

【図面の簡単な説明】

【図1】本発明のセキュリティ管理装置の適用対象となるオープン型の分散ネットワークシステムの一例を示す図である。

【図2】本発明のセキュリティ管理装置におけるセキュリティポリシーの一例を示す図である。

【図3】本発明のセキュリティ管理装置の一実施例を構成するセキュリティメッセージ抽出手段による処理の概要を示す図である。

【図4】本発明のセキュリティ管理装置の一実施例を構成するセキュリティメッセージ分析手段による処理の概要を示す図である。

【図5】本発明のセキュリティ管理装置の一実施例を構成するセキュリティメッセージ選択収集手段による処理の概要を示す図である。

【図6】本発明のセキュリティ管理装置の一実施例を構成するセキュリティメッセージ記録手段による処理の概要を示す図である。

12

【図7】図3～図6の各処理の対象とされるデータ群の形式の一例を示す図である。

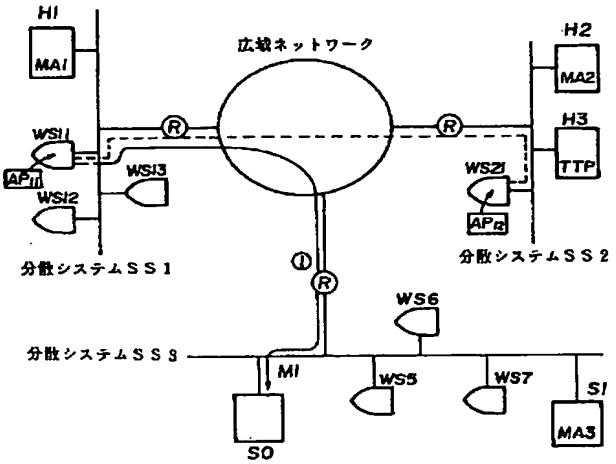
【図8】本発明のセキュリティ管理装置の一実施例を構成するセキュリティレポート分析手段およびセキュリティポリシー診断手段による処理の概要を示す図である。

【図9】本発明のセキュリティ管理装置の一実施例を構成するセキュリティポリシー改変要求手段による処理の概要を示す図である。

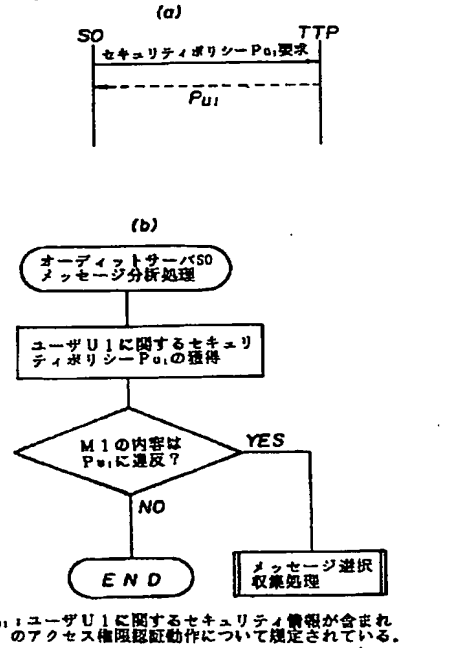
【符号の説明】

SO　セキュリティオーディットサーバ
H1，H2，....　ホストシステム
WS1，WS2，....　ワークステーション
SS1，SS2，....　分散システム
MA1，MA2，MA3　ネットワークマネジャ
AP1，AP2，....　アプリケーションプログラム
TTP　Trusted Third Party
U1　ユーザ
M1　セキュリティ侵害メッセージ
P，P_{U1}　セキュリティポリシー
R，R1　セキュリティレポート

【図1】



【図4】



P_{U1}：ユーザU1に関するセキュリティ情報が含まれ U_1 のアクセス権限認証動作について規定されている。

【図2】

【図２】セキュリティポリシーの一例

(a)

Pのパラメタ表現
ネットワークマネジャ名称
認証レベル
アクセス制御レベル
完全性レベル
機密性レベル
オーディットレベル
:
:

(b)

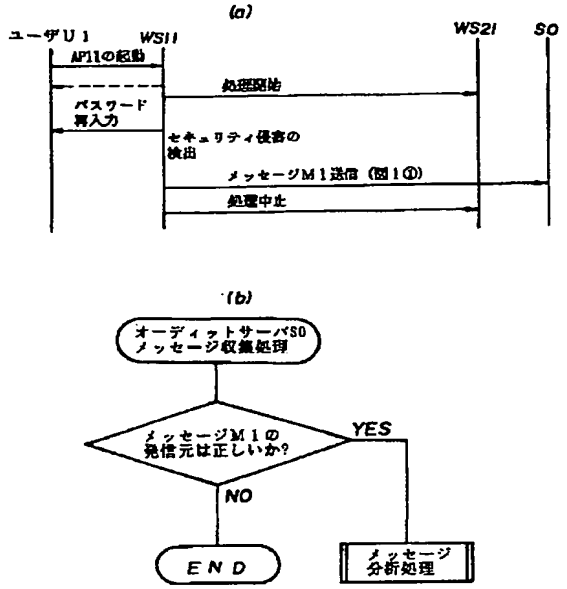
P_{U_1}の値	
ネットワークマネジャ名称	MA_1
認証レベル	Au－2
アクセス制御レベル	Ac－2
完全性レベル	In－0
機密性レベル	Cn－4
オーディットレベル	Ad－3
:	
:	

(凡例)
認証レベル　Au－0：認証を行わない
1：ログイン時のみの認証
2：定期的にパスワード入力による認証

アクセス制御レベル　Ac－0：アクセス制御を行わない
1：自システム内のみのアクセス制御
2：他システムも含んだアクセス制御

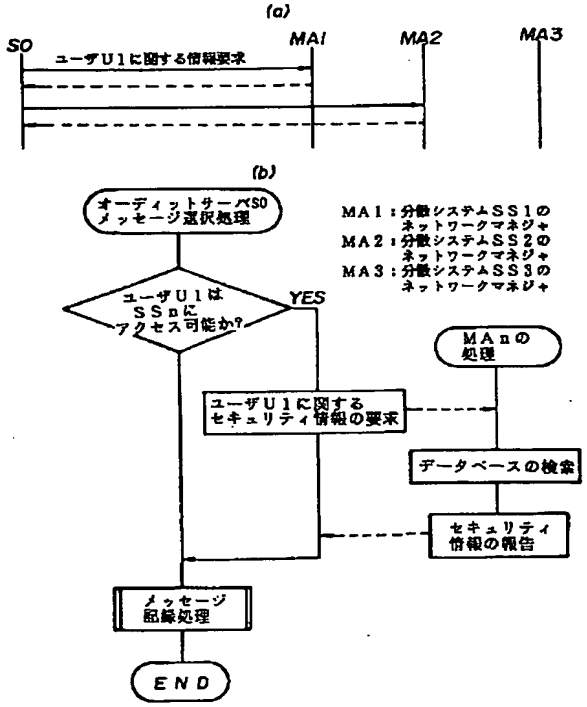
【図3】

【図３】セキュリティメッセージ抽出手段による処理の概要



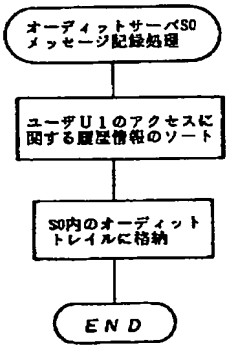
【図5】

【図５】
セキュリティメッセージ選択収集手段による処理の概要



【図6】

【図６】
セキュリティメッセージ記録手段による処理の概要



【図7】

【図７】 データ群の形式の一例

(a)

IDO1 USER U1 REGLECTED PASSWORD AUTENTICATION

(b)

セキュリティポリシー	セキュリティメッセージ	日時	付加情報
P_{u1}	M1	Y1M1D1	OK
P_{u1} :	M1 :	Y2M2D2 :	NG :

(c)

ユーザ	セキュリティメッセージ	日時	アクセス履歴
U1	M1	$Y_\alpha M_\alpha D_\alpha$	SS1
U2 :	M2 :	$Y_\beta M_\beta D_\beta$:	SS1 :

(d)

ユーザ	セキュリティメッセージ	日時	アクセス履歴	付加情報
U1	M1	$Y_\alpha M_\alpha D_\alpha$	SS1	OK
U1	M3	$Y_\gamma M_\gamma D_\gamma$	SS2	OK
U1 :	M7 :	$Y_\varphi M_\varphi D_\varphi$:	SS3 :	NG :

(e)

ユーザU1

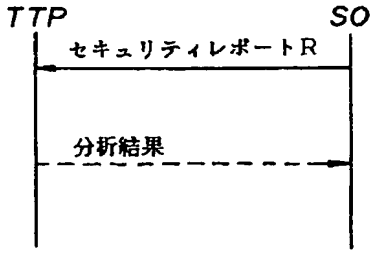
ymd	time	アクセス履歴	可否
19920914	10:00	SS1	OK
:		:	:
:		:	:
		SS2	NG
		SS3	OK

【図8】

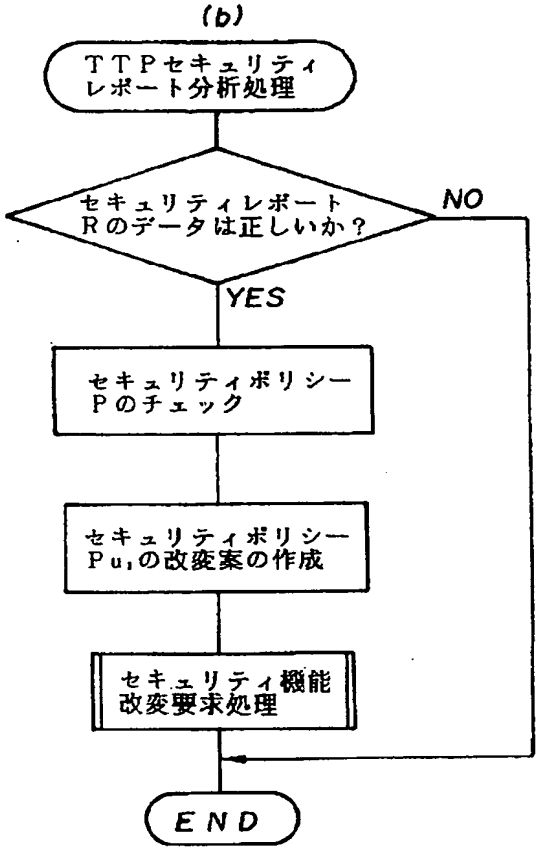
【図８】

セキュリティレポート分析手段および
セキュリティポリシー診断手段による処理の概要

(a)

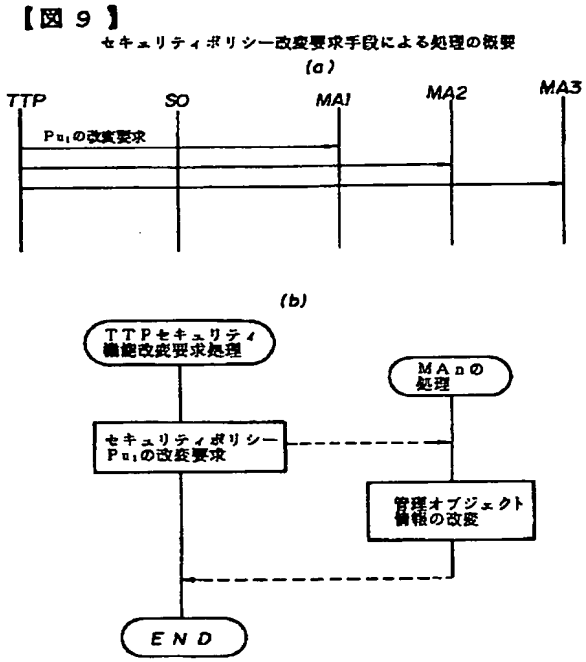


(b)



【図9】

【図９】



フロントページの続き

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｌ	9/10				
	9/12				